Format Examples

US Patent
US6024053 or 6024053

US Design Patent
D0318249

US Plant Patents
PP8901

US Reissue
RE35312

US SIR
H1523

US Patent Applications
20020012233

World Patents
WO04001234 or WO2004012345

European
EP1067252

Great Britain
GB2018332

German
DE29980239

Nerac Document Number (NDN)
certain NDN numbers can be used for patents

view examples

Patent Abstract

GER 2003-05-08 10146821
ZUTRITTSKONTROLLSYSTEM

INVENTOR- GILGE MICHAEL DE

APPLICANT- VCS VIDEO COMM SYSTEMS AG DE
PATENT NUMBER- 10146821/DE-A1
PATENT APPLICATION NUMBER- 10146821
DATE FILED- 2001-09-20
DOCUMENT TYPE- A1, DOCUMENT LAID OPEN (FIRST PUBLICATION)
PUBLICATION DATE- 2003-05-08
INTERNATIONAL PATENT CLASS- G07C00900
PATENT APPLICATION PRIORITY- 10146821, A
PRIORITY COUNTRY CODE- DE, Germany, Ged. Rep. of
PRIORITY DATE- 2001-09-20
FILING LANGUAGE- German
LANGUAGE- German NDN- 203-0514-6876-7

EXEMPLARY CLAIMS- 1. Access control system to the building or area access control, comprehensively: at least one data acquisition mechanism (18), which entrance (16), which can be controlled at one, is arranged; a communication device (38), which is assigned to one or more data acquisition mechanisms (18) and over the seized data to a digital net (44; 48) is transferable; a checking device (26), by which the seized data are evaluable and at least one communication device (50), which is assigned to the checking device (26) and over the data from the digital net (44, sent by the data acquisition communication device (38); 48) is receiptable. 2. Access control system according

to requirement 1,by the fact chara[redacted]zed that a digital net (44; 48) an before-existing net independent of the access control system is. 3. Access control system according to requirement 1 or 2, by the fact characterized that a digital net is a public net (44). 4. Access control system after one of the preceding requirements, by the fact characterized that a digital net is the InterNet, a ISDNNetz, a GSM net or a UMTS net. 5. Access control system after one of the preceding requirements, by the fact characterized that a digital net is a proprietaeres net (48). 6. Access control system after one of the preceding requirements, by the fact characterized that a digital net is a local area network or not-local net. 7. Access control system after one of the preceding requirements, by the fact characterized that the data acquisition mechanism (18) covers a camera (20) for the collection of graphic datafor the admission control. 8. Access control system after one of the preceding requirements, by the fact characterized that the data acquisition mechanism (18) covers a document reader. 9. Access control system after one of the preceding requirements, by the fact characterized that the data acquisition mechanism (18) covers a microphone (22) for the collection of acousticdata for the admission control. 10.

NO-DESCRIPTORS

Nerac, Inc. One Technology Drive . Tolland, CT
Phone (860) 872-7000 Fax (860) 875-1749

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 46 821 A 1**

(51) Int. Cl.[7]: **G 07 C 9/00**

(21) Aktenzeichen: 101 46 821.0
(22) Anmeldetag: 20. 9. 2001
(43) Offenlegungstag: 8. 5. 2003

(71) Anmelder:
VCS Video Communication Systems AG, 90425 Nürnberg, DE

(74) Vertreter:
HOEGER, STELLRECHT & PARTNER PATENTANWÄLTE, 70182 Stuttgart

(72) Erfinder:
Gilge, Michael, Dr., 90408 Nürnberg, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Zutrittskontrollsystem

(57) Um ein Zutrittskontrollsystem zur Gebäude- oder Geländezugangskontrolle zu schaffen, welches flexibel einsetzbar ist und mit dem sich insbesondere eine Mehrzahl von Zugängen kontrollieren läßt, ist vorgesehen, daß das Zutrittskontrollsystem mindestens eine Datenerfassungseinrichtung umfaßt, welche an einem zu kontrollierenden Zugang angeordnet ist; eine Kommunikationseinrichtung umfaßt, welche einer oder mehreren Datenerfassungseinrichtungen zugeordnet ist und über die erfaßten Daten an ein digitales Netz übertragbar sind; eine Kontrolleinrichtung umfaßt, durch welche die erfaßten Daten auswertbar sind und mindestens eine Kommunikationseinrichtung umfaßt, welche der Kontrolleinrichtung zugeordnet ist und über die von der Datenerfassungs-Kommunikationseinrichtung gesendete Daten aus dem digitalen Netz empfangbar sind.

DE 101 46 821 A 1

DE 101 46 821 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Zutrittskontrollsystem zur Gebäude- oder Geländezugangskontrolle.

[0002] Solche Zutrittskontrollsysteme werden üblicherweise so aufgebaut, daß eine Datenerfassungseinrichtung fest mit einer lokalen Kontrolleinrichtung verdrahtet ist.

[0003] Der Erfindung liegt die Aufgabe zugrunde, ein Zutrittskontrollsystem zu schaffen, welches flexibel einsetzbar ist und mit dem sich insbesondere eine Mehrzahl von Zugängen kontrollieren läßt.

[0004] Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß mindestens eine Datenerfassungseinrichtung vorgesehen ist, welche an einem zu kontrollierenden Zugang angeordnet ist; eine Kommunikationseinrichtung vorgesehen ist, welche einer oder mehreren Datenerfassungseinrichtungen zugeordnet ist und über die erfaßte Daten an ein digitales Netz übertragbar sind; eine Kontrolleinrichtung vorgesehen ist, durch welche die erfaßten Daten auswertbar sind; und mindestens eine Kommunikationseinrichtung vorgesehen ist, welche der Kontrolleinrichtung zugeordnet ist und über die von der Datenerfassungs-Kommunikationseinrichtung gesendete Daten aus dem digitalen Netz empfangbar sind.

[0005] Über die Übertragung von Daten auf dem digitalen Netz läßt sich die Kontrolleinrichtung räumlich entkoppeln von dem Zugang bzw. von den einzelnen Zugängen. Die Auswertung bzw. die Freigabe eines Zugangs läßt sich damit zentral durchführen, beispielsweise in einer Firmenzentrale, ohne daß jedem einzelnen Zugang eine eigene Kontrolleinrichtung zugeordnet werden muß. Beispielsweise läßt sich zu Zeiten, in denen die Zugangsfrequenz niedrig ist, über eine Firmenzentrale der Zutritt an verschiedenen Firmensitzen kontrollieren.

[0006] Dadurch, daß ein digitales Netz als Übertragungsweg zwischen den Zugängen und der Kontrolleinrichtung verwendet wird, läßt sich auch der Verdrahtungsaufwand minimieren.

[0007] Insbesondere ist dabei das digitale Netz ein vorexistierendes, von dem Zutrittskontrollsystem unabhängiges Netz. Es muß damit keine physikalische Verbindung zwischen einem Zugang und der Kontrolleinrichtung neu hergestellt werden, sondern es genügt, entsprechende Kommunikationseinrichtungen vorzusehen, welche für die Ankopplung der Datenerfassungseinrichtung an dieses Netz und für die Ankopplung der Kommunikationseinrichtung an dieses Netz sorgen.

[0008] Es kann sich bei dem nichtlokalen digitalen Netz beispielsweise um ein öffentliches Netz handeln. Beispiele für solch ein Netz sind das Internet, ein ISDN-Netz, ein GSM-Netz oder ein UMTS-Netz.

[0009] Es kann sich aber auch um ein proprietäres Netz handeln, welches beispielsweise über geleaste Leitungen gebildet ist. Ein Beispiel für solche ein Netz ist ein firmeneigenes Intranet.

[0010] Bei dem digitalen Netz kann es sich um ein lokales Netz (LAN – Local Area Network) handeln oder um ein nichtlokales Netz (WAN – Wide Area Network).

[0011] Ganz besonders vorteilhaft ist es, wenn die Datenerfassungseinrichtung eine Kamera zur Erfassung von Bilddaten für die Zutrittskontrolle umfaßt. Dadurch lassen sich direkt Bilder von der Zugang suchenden Person an die Kontrolleinrichtung übertragen.

[0012] Ferner kann es vorgesehen sein, daß die Datenerfassungseinrichtung einen Dokumentenleser umfaßt, mit dem insbesondere Identifikationsdokumente lesbar sind, um so entsprechende Identifikationsdaten an die Kontrolleinrichtung übertragen zu können.

[0013] Ferner kann es vorgesehen sein, daß die Datenerfassungseinrichtung ein Mikrofon zur Erfassung akustischer Daten für die Zutrittskontrolle umfaßt. Dadurch kann die Kontrolleinrichtung mindestens unidirektional mit einer Zugang suchenden Person kommunizieren.

[0014] Ganz besonders vorteilhaft ist es, wenn ein oder mehrere Analog-/Digital-Wandler vorgesehen sind, mit dem oder denen erfaßte Daten in Digitalsignale zur Übertragung auf dem digitalen Netz umwandelbar sind. Beispielsweise liefern eine Kamera oder ein Mikrofon analoge Signale, die zuerst gewandelt werden müssen, damit sie beispielsweise im Internet übertragbar sind.

[0015] In dieser Hinsicht ist es besonders günstig, wenn eine Bilddatenvorrichtung vorgesehen ist, welche von einer Kamera und/oder einem Mikrofon der Datenerfassungseinrichtung gelieferte Bilddaten/akustische Daten in für die Übertragung auf dem digitalen Netz geeignete Daten umwandelt. Diese Bilddatenvorrichtung kann dazu verwendet werden, um die Datenerfassungseinrichtung an das digitale Netz zu koppeln. Sie liefert die Daten in dem Format, wie sie auf dem digitalen Netz übertragbar sind. Mittels ihr läßt sich auch ein bereits vorhandenes Zutrittskontrollsystem in ein erfindungsgemäßes Zutrittskontrollsystem umrüsten, indem entsprechend die Analogdaten zur Übertragung auf dem digitalen Netz gewandelt werden.

[0016] Vorteilhafterweise umfaßt die Bilddatenvorrichtung einen Analog-/Digital-Wandler zur Umwandlung von analogen Bilddaten/akustischen Daten in digitale Bilddaten/akustische Daten, um die Übertragbarkeit der Daten auf einem digitalen Netz zu ermöglichen.

[0017] Ferner ist es vorgesehen, daß die Bilddatenvorrichtung einen Komprimierer umfaßt, welcher digitale Bilddaten/akustische Daten in ein geeignetes Format komprimiert wie beispielsweise JPEG, MPEG-2, MPEG-4 oder H.323. Das Datenformat wird dabei je nach erforderlicher Anwendung gewählt unter Berücksichtigung der Randbedingungen wie beispielsweise Bandbreite.

[0018] Weiterhin ist es vorgesehen, daß die Bilddatenvorrichtung Bilddaten/akustische Daten paketweise zusammenfaßt und an ein Netzwerkprotokoll anpaßt. Dadurch wird die Übertragung auf dem digitalen Netz an die Kommunikationseinrichtung ermöglicht.

[0019] Insbesondere ist die Bilddatenvorrichtung an ein lokales Netzwerk gekoppelt, an welches die Datenerfassungs-Kommunikationseinrichtung ebenfalls gekoppelt ist. Über das lokale Netzwerk lassen sich dann die entsprechenden Daten lokal speichern. Darüber hinaus lassen sie sich durch die Kommunikationseinrichtung speichern. Damit liegen zwei Datensätze vor, nämlich zum einen ein lokal gespeicherter Datensatz und zum anderen ein bei der Kommunikationseinrichtung gespeicherter Datensatz. Dadurch läßt sich redundant ermitteln, welchen Personen der Zutritt gewährt wurde, so daß wiederum bestimmbar ist, wieviele und welche Personen sich in einem Gebäude oder auf einem Gelände aufhalten. Solche Daten können während eines Notfalls von entscheidender Bedeutung sein.

[0020] Günstigerweise weist die Bilddatenvorrichtung Kontrolleinrichtungsfunktionen auf, so daß durch diese erfaßte Daten auswertbar sind. Es lassen sich dann Identifikationsverfahren wie die Prüfung von Zugangsausweisen und/oder Gesichtserkennungsverfahren lokal von der Bilddatenvorrichtung durchführen.

[0021] Erfindungsgemäß ist durch die Kontrolleinrichtung eine Mehrzahl von Zugängen kontrollierbar. Die Kontrolleinrichtung kann erfindungsgemäß die Daten einer Mehrzahl von Zugängen empfangen, wobei es auf die räumliche Trennung nicht ankommt. Dadurch kann durch eine einzige Kontrolleinrichtung oder durch wenige Kontrolleinrichtun-

gen eine Vielzahl von Zugängen überwacht werden, wodurch wiederum beispielsweise zu wenig frequentierten Zeiten eine zentrale Zutrittskontrolle ermöglichst wird. Insbesondere ist dabei die Kontrolleinrichtung eine zentrale Einrichtung, welche beispielsweise einer Firmenzentrale zugeordnet ist.

[0022] Ferner ist es günstig, wenn die Kontrolleinrichtung einen Speicher für Zugangsdaten umfaßt oder mit einem solchen Speicher verbunden ist. Dadurch lassen sich dann die Daten von Personen speichern, denen Zutritt gewährt wurde, um so beispielsweise zu jedem Zeitpunkt die Anzahl der in einem Gebäude oder auf einem Gelände befindlichen Personen ermitteln zu können.

[0023] Ferner kann es vorgesehen sein, daß die Kontrolleinrichtung Auswertungseinrichtungen umfaßt. Mit solchen Auswertungseinrichtungen sind Identifikationsverfahren wie beispielsweise ein Gesichtserkennungsverfahren durchführbar, um so eine sichere und vorzugsweise automatische Zutrittskontrolle zu ermöglichen.

[0024] Es ist ferner vorgesehen, daß durch die Kontrolleinrichtung einem Zugang Steuerbefehle zur Zugangsöffnung/Zugangsverweigerung übermittelbar sind. Hat eine Auswertung durch die Kontrolleinrichtung ergeben, daß einer Zugang suchenden Person Zutritt gewährt werden kann, dann übermittelt günstigerweise die Kontrolleinrichtung entsprechende Steuerbefehle, um den Zugang zu öffnen.

[0025] Die Erfindung betrifft ferner eine Bilddatenvorrichtung für ein Zutrittskontrollsystem.

[0026] Hier liegt die Aufgabe zugrunde, eine Bilddatenvorrichtung zu schaffen, mittels welcher sich unter Minimierung des Verdrahtungsaufwands erfaßte Daten an eine räumlich getrennte Kontrolleinrichtung übertragbar sind.

[0027] Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß die Bilddatenvorrichtung an eine Datenerfassungseinrichtung des Zutrittskontrollsystem koppelbar ist und so an ein digitales Netz koppelbar ist, daß von der Datenerfassungseinrichtung erfaßte Daten an das digitale Netz übertragbar sind, wobei Bilddaten/akustische Daten der Datenerfassungseinrichtung in ein auf dem digitalen Netz übertragbares Datenformat umwandelbar sind, so daß durch eine mit dem digitalen Netz verbundene Kontrolleinrichtung diese Daten auswertbar sind.

[0028] Diese Bilddatenvorrichtung weist die bereits im Zusammenhang mit dem erfindungsgemäßen Zutrittskontrollsystem erläuterten Vorteile auf.

[0029] Weitere vorteilhafte Ausgestaltungen wurden ebenfalls bereits im Zusammenhang mit dem erfindungsgemäßen Zutrittskontrollsystem erläutert.

[0030] Insbesondere ist es vorteilhaft, wenn die erfaßten Daten in ein bestimmtes Format komprimierbar sind, so daß unter Nutzung der Bandbreite des digitalen Netzes für die Zutrittskontrolle optimierte Daten an die Kontrolleinrichtung übertragbar sind.

[0031] Aus dem gleichen Grund ist es günstig, wenn die Daten paketweise zusammenfaßbar sind und die Daten an ein bestimmtes Protokoll anpaßbar sind.

[0032] Insbesondere ist es vorgesehen, daß die Bilddatenvorrichtung an ein lokales digitales Netz koppelbar ist, um die entsprechenden Daten auch dem lokalen digitalen Netz bereitzustellen. Die erfaßten Daten können dann ebenfalls vor Übertragung an die Kontrolleinrichtung in einem entsprechenden Zugangsstrang, welcher das lokale digitale Netz umfaßt, gespeichert werden.

[0033] Die Erfindung betrifft ferner eine Kontrolleinrichtung für ein Zutrittskontrollsystem.

[0034] Hier liegt die Aufgabe zugrunde, eine Kontrolleinrichtung zu schaffen, mittels welcher eine Mehrzahl von Zugängen überwachbar ist.

[0035] Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß die Kontrolleinrichtung an ein digitales Netz koppelbar ist, so daß von einer einem Zugang zugeordneten Datenerfassungseinrichtung auf dem digitalen Netz gesendete Daten empfangbar und auswertbar sind.

[0036] Durch solch eine Kontrolleinrichtung, die räumlich trennbar ist von den Zugängen, lassen sich dann also die entsprechenden gesendeten Daten erfassen und auswerten und so wiederum lassen sich Zugänge freigeben bzw. sperren.

[0037] Diese Kontrolleinrichtung weist die bereits im Zusammenhang mit dem erfindungsgemäßen Zutrittskontrollsystem und der erfindungsgemäßen Bilddatenvorrichtung erläuterten Vorteile auf.

[0038] Weitere vorteilhafte Ausgestaltungen wurden ebenfalls bereits im Zusammenhang mit dem erfindungsgemäßen Zutrittskontrollsystem und der erfindungsgemäßen Bilddatenvorrichtung erläutert.

[0039] Die nachfolgende Beschreibung einer bevorzugten Ausführungsform der Erfindung dient im Zusammenhang mit der Zeichnung der näheren Erläuterung der Erfindung. In der einzigen

[0040] **Fig. 1** ist eine schematische Darstellung eines Ausführungsbeispiels eines erfindungsgemäßen Zutrittskontrollsystems gezeigt.

[0041] Ein erfindungsgemäßes Zutrittskontrollsystem, von dem in **Fig. 1** ein Ausführungsbeispiel gezeigt und dort als Ganzes mit **10** bezeichnet ist, umfaßt mindestens einen Zugangsstrang **12** und bevorzugterweise eine Mehrzahl von Zugangssträngen **12** und einen räumlich davon getrennten Kontrollstrang **14**. Ein Zugangsstrang **12** ist dabei jeweils einem zu kontrollierenden Zugang **16** zugeordnet. Über einen solchen Zugang **16** wird der Zutritt von insbesondere Personen und/oder Fahrzeugen zu einem Gebäude oder zu einem Gelände kontrolliert.

[0042] Einem Zugang ist jeweils mindestens eine Datenerfassungseinrichtung **18** zugeordnet, welche die zur Identifizierung von Zutritt suchenden Personen notwendigen Daten aufnimmt. Eine solche Datenerfassungseinrichtung **18** ist daher in enger räumlicher Nähe zu dem zu kontrollierenden Zugang **16** positioniert. Eine Datenerfassungseinrichtung **18** umfaßt dabei eine Kamera **20**, um Bilddaten zu erzeugen, ein Mikrofon **22**, um akustische Daten zu liefern und gegebenfalls auch einen Kartenleser, um beispielsweise Zutrittsausweise zu lesen und somit entsprechende Identifikationsdaten erfassen zu können. Es kann darüber hinaus auch vorgesehen sein, daß die Datenerfassungseinrichtung **18** einen Lautsprecher **24** aufweist, um eine akustische bidirektionale Kommunikation zwischen einer Zutritt suchenden Person und einer Kontrolleinrichtung **26** im Kontrollstrang **14** zu ermöglichen.

[0043] Die Datenerfassungseinrichtung **18** ist insbesondere mit einem Aktivierungsschalter **28** versehen, bei dessen Aktivierung eine Zutritt suchende Person den Datenerfassungsvorgang in Gang setzt, d. h. über die Kamera **20** wird die Bilddatenaufnahme der Zutritt suchenden Person gestartet und die Erfassung akustischer Daten über das Mikrofon **22** wird initialisiert. Auf ähnliche Weise kann ein Dokumentenleser initialisiert werden, um Identifikationsdaten erfassen zu können.

[0044] Der Datenerfassungseinrichtung **18** nachgeschaltet ist eine Bilddatenvorrichtung **30**, welche die von der Datenerfassungseinrichtung **18** gelieferten Daten (Bilddaten, akustische Daten, Identifikationsdaten) verarbeitet, so daß diese über ein lokales digitales Netz (LAN – Local Area Network) und/oder ein nichtlokales digitales Netz (WAN – Wide Area Network) an den Kontrollstrang **14** übertragbar sind.

[0045] Dazu umfaßt die Bilddatenvorrichtung **30** einen Analog-/Digital-Wandler, welcher von der Datenerfas-

sungseinrichtung **18** gelieferte analoge Signale in digitale Signale umwandelt. Insbesondere werden analoge Bilddaten und analoge akustische Daten in digitale Signale umgewandelt. Die Initialisierung erfolgt dabei vorzugsweise durch Aktivierung des Aktivierungsschalters **28**, welcher über eine Leitung **32** mit der Bilddatenvorrichtung **30** verbunden ist. Ferner sind Leitungen **34** und **36** jeweils zur Verbindung der Kamera **20** und des Mikrofons **22** mit der Bilddatenvorrichtung **30** vorgesehen.

[0046] Die Bilddatenvorrichtung **30** umfaßt ferner einen Komprimierer, welcher die Bilddaten/akustischen Daten in ein bestimmtes komprimiertes Datenformat wandelt, wie beispielsweise MPEG-2, MPEG-4, JPEG oder H.323. Es sind auch weitere Datenformate möglich. Das jeweils gewählte Datenformat, mittels dessen die Signale über das digitale Netz an die Kontrolleinrichtung **26** übertragbar sind, wird je nach Anwendung gewählt. Genügt es für die Zutrittskontrolle beispielsweise, der Kontrolleinrichtung statische Bilder bereitzustellen anstatt bewegter Bilder, dann ist JPEG ein geeignetes Komprimierungsformat.

[0047] Ist es dagegen erforderlich, daß auch bewegte Bilder übertragen werden müssen, dann ist beispielsweise ein MPEG-Format vorgesehen.

[0048] Die Bilddatenvorrichtung **30** faßt ferner die Daten paketweise zusammen und versieht sie mit einem für die Übertragung auf dem digitalen Netz geeigneten Protokoll.

[0049] Die Bilddatenvorrichtung **30** ist über eine Kommunikationseinrichtung, welche in **Fig. 1** als Ganzes mit 38 bezeichnet ist, bei dem gezeigten Ausführungsbeispiel an ein nichtlokales digitales Netz über ein lokales Netz **40** mittels eines ersten Kommunikationsserver **42** gekoppelt, welcher die Verbindung dieses lokalen Netzes **40** mit einem nichtlokalen digitalen Netz wie beispielsweise dem Internet (Bezugszeichen **44**) bereitstellt. Bei dem lokalen Netz **40** und dem nichtlokalen digitalen Netz handelt es sich dabei um Netzwerke, welche unabhängig von dem Zutrittskontrollsystem **10** existieren. Bei dem Aufbau des erfindungsgemäßen Zutrittskontrollsystems **10** ist daher lediglich die Ankopplung an die präexistenten digitalen Netze **40, 44** bereitzustellen, um die Kommunikation mit der Kontrolleinrichtung **26** zu ermöglichen.

[0050] Neben dem Internet lassen sich die von der Bilddatenvorrichtung **30** gelieferten digitalen Signale auch über andere Netze an den Kontrollstrang **14** übertragen, wie beispielsweise über ein ISDN-Netz oder drahtlos über ein GSM-Netz oder UMTS-Netz.

[0051] Neben der Übertragung auf öffentlichen Netzen kann es auch vorgesehen sein, daß die erfaßten Daten über ein anderes digitales Netz wie beispielsweise über ein proprietäres nichtlokales oder lokales digitales Netz (wie beispielsweise einem firmeneigenen Intranet) übertragen werden. Dazu ist, wie in **Fig. 1** schematisch gezeigt, ein zweiter Kommunikationsserver **46** vorgesehen, welcher an ein solches digitales Netz **48** gekoppelt ist.

[0052] Es kann dabei vorgesehen sein, daß die Daten der Bilddatenvorrichtung **30** über die Kommunikationseinrichtung **38** nur über ein nichtlokales/lokales digitales Netz übertragen werden (beispielsweise nur über das Internet) oder daß mehrere Einkopplungsmöglichkeiten vorgesehen sind (beispielsweise Internet oder alternativ/zusätzlich Intranet).

[0053] Es ist dabei insbesondere vorgesehen, daß die Bilddatenvorrichtung **30** die erzeugten Daten noch verschlüsselt, um entsprechend einen verschlüsselten Datensatz beispielsweise im Internet **44** übertragen zu können. Diese Verschlüsselung kann auch der erste Kommunikationsserver **42** übernehmen.

[0054] Der Kontrollstrang **14** weist ebenfalls eine Kommunikationseinrichtung auf, welche als Ganzes mit 50 bezeichnet ist. Diese Kommunikationseinrichtung **50** ist beispielsweise wiederum an ein dem Kontrollstrang **14** zugeordnetes lokales Netz **52** gekoppelt. Die Kontrolleinrichtung **26** selber ist dann ebenfalls an dieses lokale Netz **52** gekoppelt, so daß über die Kommunikationseinrichtung **50** Daten aus dem nichtlokalen digitalen Netz, wie beispielsweise dem Internet **44**, mittels des lokalen Netzes **52** an die Kontrolleinrichtung **26** übertragbar sind.

[0055] Bei dem in **Fig. 1** gezeigten Ausführungsbeispiel ist mit dem lokalen Netz **52** ein Kommunikationsserver **54** verbunden, welcher aus dem Internet **44** die von der Bilddatenvorrichtung **30** an die Kontrolleinrichtung **26** übermittelten Daten ausliest und auf dem lokalen Netz **52** an die Kontrolleinrichtung **26** weiterleitet.

[0056] Es kann alternativ oder zusätzlich ein Kommunikationsserver **56** vorgesehen sein, welcher Daten aus dem digitalen Netz **48** ausliest und an die Kontrolleinrichtung **26** überträgt.

[0057] In der Kontrolleinrichtung **26** werden die von der Datenerfassungseinrichtung **18** erfaßten Daten ausgewertet. Es kann sich dabei um eine Operator-geführte Identifikationsauswertung, automatische Auswertung oder halbautomatische Auswertung handeln. Beispielsweise umfaßt die Kontrolleinrichtung **26** Gesichtserkennungssoftware, mit deren Hilfe von der Kamera **20** gelieferte Bilddaten mit gespeicherten Bilddaten verglichen werden. Dazu ist die Kontrolleinrichtung **26** mit Speichern **58** verbunden, welche insbesondere über das lokale Netz **52** zugreifbar sind.

[0058] Ferner kann es vorgesehen sein, daß die Kontrolleinrichtung **26** Identifikationsdaten, welche mit dem Dokumentenleser der Datenerfassungseinrichtung **18** ausgelesen werden, mit vorgespeicherten Daten vergleicht. Insbesondere ist es vorgesehen, daß eine Verknüpfung zwischen Gesichtserkennung und Dokumenten-Identifikationserkennung durchgeführt wird.

[0059] Die Bilddatenvorrichtung **30** kann ebenfalls Kontrolleinrichtungsfunktionen implementiert haben, so daß durch diese eine lokale Identifikation durchführbar ist, und zwar ohne Beteiligung des Kontrollstrangs **14**.

[0060] Mittels des Lautsprechers **24** kann ein Operator mit einer Zugang suchenden Person auch bidirektional kommunizieren.

[0061] Die Kontrolleinrichtung **26** (oder gegebenenfalls die Bilddatenvorrichtung **30**) liefert in Abhängigkeit von einer Entscheidung des Operators bzw. einem Analyseergebnis Steuerbefehle an den Zugang **16**, d. h. je nach Ergebnis des Datenvergleichs wird der Zugang **16** geöffnet bzw. bleibt verschlossen. Gegebenenfalls wird beim Fehlschlagen eines Erkennungsprozesses eine Alarmprozedur in Gang gesetzt.

[0062] Durch das erfindungsgemäße Zutrittskontrollsystem **10** läßt sich durch eine zentrale Kontrolleinrichtung **26** ein räumlich getrennter Zugang **16** überwachen, wobei die räumliche Distanz aufgrund der Datenübertragung über das lokale oder nichtlokale digitale Netz beliebig sein kann. Insbesondere lassen sich über eine einzige Kontrolleinrichtung **26** eine Mehrzahl von Zugängen **16** überwachen, wobei auch diese Zugänge räumlich verstreut sein können. Damit kann also zentral, beispielsweise in einer Firmenzentrale, der Zugang an einer Mehrzahl von verschiedenen Firmensitzen überwacht werden.

[0063] Wird eine Zugangskontrolle durch die Kontrolleinrichtung **26** durchgeführt, dann werden insbesondere die ermittelten Daten gespeichert, so daß grundsätzlich die Kontrolleinrichtung **26** zu jedem Zeitpunkt die Information hat, welche Personen einen Zugang **16** passiert haben und damit wie viele und welche Personen sich in einem Gebäude bzw.

auf einem Gelände aufhalten.

[0064] Der Verkabelungsaufwand zur Ausbildung eines Zutrittskontrollsystems **10** läßt sich minimieren, da nicht jedem Zugang **16** eine eigene Kontrolleinrichtung **26** zugeordnet werden muß. Darüber hinaus wird die Verkabelung für die Übertragung von Daten von dem Zugangsstrang **12** auf den Kontrollstrang **14** und in der Gegenrichtung vermieden, da hier vorexistierende Netze verwendet werden.

[0065] Die Verbindung zwischen Zugangsstrang **12** und Kontrollstrang **14** läßt sich redundant ausbilden, indem beispielsweise neben dem Internet **44** als Aushilfsnetz noch ein Telefon-ISDN-Netz vorgesehen wird oder ein GSM-Netz.

Patentansprüche

1. Zutrittskontrollsystem zur Gebäude- oder Geländezugangskontrolle, umfassend:
mindestens eine Datenerfassungseinrichtung (**18**), welche an einem zu kontrollierenden Zugang (**16**) angeordnet ist;
eine Kommunikationseinrichtung (**38**), welche einer oder mehreren Datenerfassungseinrichtungen (**18**) zugeordnet ist und über die erfaßte Daten an ein digitales Netz (**44**; **48**) übertragbar sind;
eine Kontrolleinrichtung (**26**), durch welche die erfaßten Daten auswertbar sind und
mindestens eine Kommunikationseinrichtung (**50**), welche der Kontrolleinrichtung (**26**) zugeordnet ist und über die von der Datenerfassungs-Kommunikationseinrichtung (**38**) gesendete Daten aus dem digitalen Netz (**44**; **48**) empfangbar sind.

2. Zutrittskontrollsystem nach Anspruch 1, dadurch gekennzeichnet, daß ein digitales Netz (**44**; **48**) ein vorexistierendes, von dem Zutrittskontrollsystem unabhängiges Netz ist.

3. Zutrittskontrollsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß ein digitales Netz ein öffentliches Netz (**44**) ist.

4. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß ein digitales Netz das Internet, ein ISDN-Netz, ein GSM-Netz oder ein UMTS-Netz ist.

5. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß ein digitales Netz ein proprietäres Netz (**48**) ist.

6. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß ein digitales Netz ein lokales Netz oder nichtlokales Netz ist.

7. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Datenerfassungseinrichtung (**18**) eine Kamera (**20**) zur Erfassung von Bilddaten für die Zutrittskontrolle umfaßt.

8. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Datenerfassungseinrichtung (**18**) einen Dokumentenleser umfaßt.

9. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Datenerfassungseinrichtung (**18**) ein Mikrofon (**22**) zur Erfassung akustischer Daten für die Zutrittskontrolle umfaßt.

10. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß ein oder mehrere Analog-/Digital-Wandler vorgesehen sind, mit dem oder denen erfaßte Daten in Digitalsignale zur Übertragung auf dem digitalen Netz umwandelbar sind.

11. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß eine Bilddatenvorrichtung (**30**) vorgesehen ist, welche von einer Kamera (**20**) und/oder einem Mikrofon (**22**) der Datenerfassungseinrichtung (**18**) gelieferte Bilddaten/akustische Daten in für die Übertragung auf dem digitalen Netz geeignete Daten umwandelt.

12. Zutrittskontrollsystem nach Anspruch 11, dadurch gekennzeichnet, daß die Bilddatenvorrichtung einen Analog-/Digital-Wandler zur Umwandlung von analogen Bilddaten/akustischen Daten in digitale Bilddaten/akustische Daten umfaßt.

13. Zutrittskontrollsystem nach Anspruch 12, dadurch gekennzeichnet, daß die Bilddatenvorrichtung (**30**) einen Komprimierer umfaßt, welcher digitale Bilddaten/akustische Daten in ein geeignetes Format komprimiert.

14. Zutrittskontrollsystem nach Anspruch 12 oder 13, dadurch gekennzeichnet, daß die Bilddatenvorrichtung (**30**) Bilddaten/akustische Daten paketweise zusammenfaßt und an ein Netzwerkprotokoll anpaßt.

15. Zutrittskontrollsystem nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, daß die Bilddatenvorrichtung (**30**) an ein lokales Netzwerk (**40**) gekoppelt ist, an welches die Datenerfassungs-Kommunikationseinrichtung (**38**) ebenfalls gekoppelt ist.

16. Zutrittskontrollsystem nach einem der Ansprüche 11 bis 15, dadurch gekennzeichnet, daß die Bilddatenvorrichtung (**30**) Kontrolleinrichtungsfunktionen aufweist, so daß durch diese erfaßte Daten auswertbar sind.

17. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß durch die Kontrolleinrichtung (**26**) eine Mehrzahl von Zugängen (**16**) kontrollierbar ist.

18. Zutrittskontrollsystem nach Anspruch 17, dadurch gekennzeichnet, daß die Kontrolleinrichtung (**26**) eine zentrale Einrichtung ist.

19. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Kontrolleinrichtung einen Speicher (**58**) für Zugangsdaten umfaßt oder mit einem solchen Speicher verbunden ist.

20. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Kontrolleinrichtung (**26**) Auswertungseinrichtungen umfaßt.

21. Zutrittskontrollsystem nach Anspruch 20, dadurch gekennzeichnet, daß durch die Kontrolleinrichtung (**26**) Identifikationsverfahren durchführbar sind.

22. Zutrittskontrollsystem nach Anspruch 21, dadurch gekennzeichnet, daß durch die Kontrolleinrichtung (**26**) ein Gesichtserkennungsverfahren durchführbar ist.

23. Zutrittskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß durch die Kontrolleinrichtung (**26**) einem Zugang (**16**) Steuerbefehle zur Zugangsöffnung/Zugangsverweigerung übermittelbar sind.

24. Bilddatenvorrichtung für ein Zutrittskontrollsystem (**10**), welche an eine Datenerfassungseinrichtung (**18**) des Zutrittskontrollsystems (**10**) koppelbar ist und welche so an ein digitales Netz (**44**; **48**) koppelbar ist, daß von der Datenerfassungseinrichtung (**18**) erfaßte Daten an das digitale Netz übertragbar sind, und durch die Bilddaten/akustische Daten der Datenerfassungseinrichtung (**18**) in ein auf dem digitalen Netz (**44**; **48**) übertragbares Datenformat umwandelbar sind, so daß durch eine mit dem digitalen Netz (**44**; **48**) verbundene

Kontrolleinrichtung (26) diese Daten auswertbar sind.

25. Bilddatenvorrichtung nach Anspruch 24, dadurch gekennzeichnet, daß die erfaßten Daten in ein bestimmtes Format komprimierbar sind.

26. Bilddatenvorrichtung nach Anspruch 24 oder 25, dadurch gekennzeichnet, daß die Daten paketweise zusammenfaßbar sind.

27. Bilddatenvorrichtung nach einem der Ansprüche 24 bis 26, dadurch gekennzeichnet, daß die Daten an ein bestimmtes Protokoll anpaßbar sind.

28. Bilddatenvorrichtung nach einem der Ansprüche 24 bis 27, dadurch gekennzeichnet, daß die Bilddatenvorrichtung an ein lokales digitales Netz (40) koppelbar ist.

29. Bilddatenvorrichtung nach einem der Ansprüche 24 bis 28, dadurch gekennzeichnet, daß die Bilddatenvorrichtung Kontrolleinrichtungsfunktionen aufweist.

30. Kontrolleinrichtung für ein Zutrittskontrollsystem, welche an ein digitales Netz (44; 48) koppelbar ist, so daß von einer einem Zugang (16) zugeordneten Datenerfassungseinrichtung (18) auf dem digitalen Netz (44; 48) gesendete Daten empfangbar und auswertbar sind.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 46 821 A1
Int. Cl.: G 07 C 9/00
Offenlegungstag: 8. Mai 2003

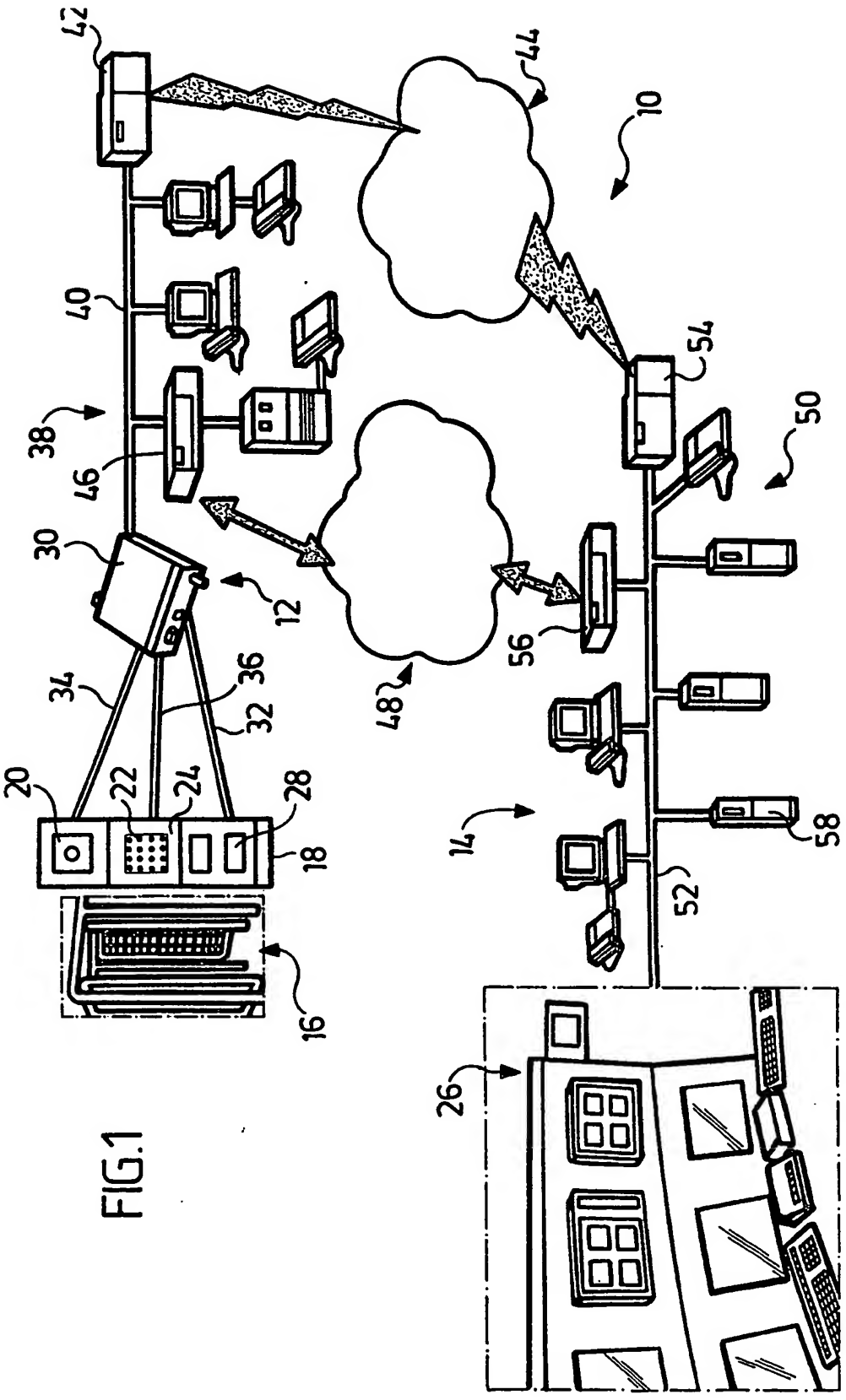

FIG.1